Order Code RS20748
Updated May 27, 2008

CRS Report for Congress

Protection of Classified Information by Congress: Practices and Proposals

Frederick M. Kaiser
Specialist in American National Government
Government and Finance Division

Summary

The protection of classified national security and other controlled information is of concern not only to the executive branch — which determines what information is to be safeguarded, for the most part[1] — but also to Congress, which uses the information to fulfill its constitutional responsibilities. It has established mechanisms to safeguard controlled information in its custody, although these arrangements have varied over time between the two chambers and among panels in each. Both chambers, for instance, have created offices of security to consolidate relevant responsibilities, although these were established two decades apart. Other differences exist at the committee level. Proposals for change, some of which are controversial, usually seek to set uniform standards or heighten requirements for access. This report will be updated as conditions require.

Current Practices and Procedures

Congress relies on a variety of mechanisms and instruments to protect classified information in its custody. These include House and Senate offices responsible for setting and implementing standards for handling classified information; detailed committee rules for controlling access to such information; a secrecy oath for all Members and employees of the House and of some committees; security clearances and nondisclosure agreements for staff; and formal procedures for investigations of suspected security violations. Public

[1] Classification of national security information is governed for the most part by executive orders E.O. 12958, issued by President William J. Clinton in 1995, and E.O. 13292, amending it, issued by President George W. Bush in 2003. Related information — such as atomic energy "Restricted Data" (42 U.S.C. 2162-2168) and "intelligence sources and methods" (50 U.S.C. 403(d)(3)) — is specified in statute and subsequent rules issued, respectively, by the Department of Energy and Director of National Intelligence. Other controlled information — such as "sensitive security" and "sensitive but unclassified" information — is determined largely by executive directives. See CRS Report RL33494, *Security Classified and Controlled Information: History, Status, and Emerging Issues*, by Harold C. Relyea; and CRS Report RS21900, *Protection of Classified Information: The Legal Framework*, by Jennifer K. Elsea.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
27 MAY 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Protection of Classified Information by Congress: Practices and Proposals	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Congressional Research Service,The Library of Congress,101 Independence Avenue SE,Washington,DC,20540-7500**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**6**	

law, House and Senate rules, and committee rules, as well as custom and practice, constitute the bases for these requirements.[2]

Chamber Offices of Security and Security Manuals

The chambers have approached their security program differently, although each now has an office of security. The Senate established an Office of Senate Security over two decades ago, in 1987, as the result of a bipartisan effort over two Congresses. It is charged with consolidating information and personnel security.[3] Located in the Office of the Secretary of the Senate, the Security Office sets and implements uniform standards for handling and safeguarding classified and other sensitive information in the Senate's possession. The Security Office's standards, procedures, and requirements — detailed in its *Senate Security Manual*, initially issued in 1988 — "are binding upon all employees of the Senate."[4] These cover committee and Member office staff and officers of the Senate as well as consultants and contract personnel. The regulations extend to a wide range of matters on safeguarding classified information: physical security requirements; procedures for storing materials; mechanisms for protecting communications equipment; security clearances and nondisclosure agreements for all Senate staff needing access; and follow-up investigations of suspected security violations by employees.

The House put its own security office in place, under the jurisdiction of the Sergeant at Arms, in 2005, following approval of the chamber's Committee on House Administration.[5] The new office, similar to the Senate predecessor, is charged with developing an Operations Security Program for the House. Its responsibilities and jurisdiction encompass processing security clearances for staff, handling and storing classified information, managing a counterintelligence program for the House, and coordinating security breach investigations. In the past, the House had relied on

---

[2] See Herrick S. Fox, "Staffers Find Getting Security Clearances Is Long and Often a Revealing Process," *Roll Call*, October 30, 2000, pp. 24-25; Frederick M. Kaiser, "Congressional Rules and Conflict Resolution: Access to Information in the House Select Committee on Intelligence," *Congress and the Presidency*, vol. 15 (1988), pp. 49-73; U.S. Commission on Protecting and Reducing Government Secrecy, *Secrecy: Report of the Commission* (1997); House Committee on Government Operations, Subcommittee on Legislation and National Security, *Congress and the Administration's Secrecy Pledges*, Hearings, 100th Cong., 2nd sess. (1988); House Permanent Select Committee on Intelligence, *United States Counterintelligence and Security Concerns — 1986*, 100th Cong., 1st sess., H.Rept. 100-5 (1987), pp. 3-4; Joint Committee on the Organization of Congress, *Committee Structure*, Hearings, 103rd Cong., 1st sess. (1993), pp. 64-79, 312-316, 406-417, and 832-841; and Senate Select Committee on Intelligence, *Meeting the Espionage Challenge*, S.Rept. 99-522, 99th Cong., 2nd sess. (1986), pp. 90-95.

[3] *Congressional Record*, vol. 133, July 1, 1987, pp. 18506-18507. The resolution creating the new office (S.Res. 243, 100th Cong.) was introduced and approved on the same day.

[4] U.S. Senate, Office of Senate Security, *Security Manual* (revised, 1998), preface.

[5] The two relevant letters — one requesting an Operations Security Program under the direction of the House Sergeant at Arms and the other granting approval — are, respectively, to the Chairman of the House Committee on House Administration, from the House Sergeant at Arms, February 25, 2003; and to the House Sergeant at Arms, from the Chairman of the House Committee on House Administration, March 28, 2003.

individual committee and Member offices to set requirements following chamber and committee rules, guidelines in internal office procedural manuals, and custom.

Security Clearances and Nondisclosure Agreements for Staff

Security clearances and written nondisclosure agreements can be required for congressional staff but have been handled differently by each chamber.[6] The Senate Office of Security mandates such requirements for all Senate employees needing access to classified information.[7] No comparable across-the-board requirements for security clearances or secrecy agreements yet exist for all House employees. But these could be applied by the new office of security, when it becomes fully operational.

Secrecy Oath for Members and Staff

The House and Senate differ with regard to secrecy oaths for Members and staff. Beginning with the 104th Congress, the House adopted a secrecy oath for all Members, officers, and employees of the chamber. Before any such person may have access to classified information, he or she must "solemnly swear (or affirm) that I will not disclose any classified information received in the course of my service with the House of Representatives, except as authorized by the House of Representatives or in accordance with its Rules" (House Rule XXIII, cl. 13, 110th Cong.).

Previously, a similar oath was required for only Members and staff of the House Permanent Select Committee on Intelligence; its requirement had been added in the 102nd Congress as part of the Select Committee's internal rules, following abortive attempts to establish it in public law.[8] It is still in effect for Members and staff: "I do solemnly swear (or affirm) that I will not disclose or cause to be disclosed any classified information in the course of my service on the [Committee], except when authorized to do so by the Committee or the Houses of Representatives" (Committee Rule 14(d), 110th Cong.). Other adoptions have occurred under committee rules. The House Committee on Homeland Security, for instance, requires an oath from each Member, officer, and employee of the committee, or a non-Member seeking access, similar to one developed by the House Intelligence Committee. Each must affirm that "I will not disclose any classified information received in the course of my service on the Committee on Homeland Security, except as authorized by the Committee or the House of Representatives or in accordance with the Rules of such Committee or the Rules of the House" (Committee Rule XIV(E), 110th Cong.). Neither the full Senate nor any Senate panel apparently imposes a similar obligation on its Members or employees.

---

[6] The congressional support agencies — i.e., Congressional Budget Office, Congressional Research Service (as well as the Library of Congress), and Government Accountability Office — have separate personnel security systems and policies. Nonetheless, each requires security clearances for its staff to gain access to classified information.

[7] Executive Order 12968, "Access to Classified Information," issued by President William Clinton, on August 2, 1995, *Federal Register*, August 7, 1995, vol. 60, pp. 240, 245-250, and 254.

[8] U.S. Congress, Committee of Conference, *Intelligence Authorization Act, Fiscal Year 1992*, 102nd Cong., 1st sess., H.Rept. 102-327 (Washington: GPO, 1991), pp. 35-36.

Investigation of Security Breaches

The Senate Office of Security and the House counterpart are charged with investigating or coordinating investigations of suspected security violations by employees. In addition, investigations by the House and Senate Ethics Committees of suspected breaches of security are authorized by each chamber's rules, directly and indirectly. The Senate Ethics Committee, for instance, has the broad duty to "receive complaints and investigate allegations of improper conduct which may reflect upon the Senate, violations of law, violations of the Senate Code of Official Conduct, and violations of rules and regulations of the Senate" (S.Res. 338, 88th Cong.). The panel is also directed "to investigate any unauthorized disclosure of intelligence information [from the Senate Intelligence Committee] by a Member, officer or employee of the Senate" (S.Res. 400, 94th Congress). The House, in creating its Permanent Select Committee on Intelligence, issued similar instructions. H.Res. 658 (95th Cong.) ordered the Committee on Standards of Official Conduct to "investigate any unauthorized disclosure of intelligence or intelligence-related information [from the House Intelligence Committee] by a Member, officer, or employee of the House...."

Sharing Information with Non-Committee Members

Procedures controlling access to classified information held by committees exist throughout Congress. These committee and chamber rules set conditions for sharing such information with other panels and Members, determining who is eligible for access to a committee's classified holdings directly, or who can be given relevant information.

The most exacting requirements along all of these lines have been developed by the House Permanent Select Committee on Intelligence; the rules are based on its 1977 establishing authority (H.Res. 658, 95th Cong.) and reinforced by intelligence oversight provisions in public law, such as the 1991 Intelligence Authorization Act (P.L. 102-88; 105 Stat. 441). The panel's controls apply to committee Members sharing classified information outside the committee itself[9] as well as to non-committee Representatives seeking access to the panel's holdings. In this case, the requester must go through a multi-stage process (Committee Rule 10, 110th Cong.). Thus, it is possible for a non-member to be denied attendance at its executive sessions or access to its classified holdings. When the House Intelligence Committee releases classified information to another panel or non-member, moreover, the recipient must comply with the same rules and procedures that govern the intelligence committee's control and disclosure requirements. By comparison, rules of the House Armed Services Committee (Committee Rule 20, 110th Cong.) "ensure access to information by any member of the Committee or any other Member, Delegate, or Resident Commissioner of the House of Representatives .... who has requested the opportunity to review such material."

Proposals for Change

A variety of proposals, coming from congressional bodies, government commissions, and other groups, have called for changes in the current procedures for handling and

---

[9] For a description of the strictures governing communications outside the House Intelligence Committee, see interview with Representative Jane Harman, "House Committee to Probe Ruin of CIA Tapes," *Morning Edition*, National Public Radio, January 16, 2008.

safeguarding classified information in the custody of Congress. These plans, some of which might be controversial or costly, focus on setting uniform standards for congressional offices and employees and heightening the access eligibility requirements.

Mandate That Members of Congress Hold Security Clearances to Be Eligible for Access to Classified Information. This would mark a significant departure from the past. Members of Congress (as with the President and Vice President, Justices of the Supreme Court, or other federal court judges) have never been required to hold security clearances. Most of the proposals along this line appeared in the late 1980s. A recent one, however, was introduced in 2006 by Representative Steve Buyer; H.Res. 747 (109th Cong.) would have required a security clearance for Members serving on the House Permanent Select Committee on Intelligence and on the Subcommittee on Defense of the House Appropriations Committee. The resolution does not specify which entity (legislative or executive branch) would conduct the background investigation or which officer (in Congress or in the executive) would adjudicate the clearances.

The broad mandate for such clearances could be applied to four different groups: (1) all Senators and Representatives, thus, in effect, becoming a condition for serving in Congress; (2) only Members seeking access to classified information, including those on panels receiving it; (3) only Members on committees which receive classified information; or (4) only those seeking access to classified information held by panels where they are not members.

Under a security clearance requirement, background investigations might be conducted by an executive branch agency, such as the Office of Personnel Management or Federal Bureau of Investigation; by a legislative branch entity, such as the House or Senate Office of Security, or the Government Accountability Office; or possibly by a private investigative firm under contract. Possible adjudicators — that is, the officials who would judge, based on the background investigation, whether applicants would be "trustworthy" and, therefore, eligible for access to classified information — could extend to the majority or minority leaders, a special panel in each chamber, a chamber officer, or even an executive branch officer, if Congress so directed.

The main goals behind this proposed change are to tighten and make uniform standards governing eligibility for access for Members. Proponents maintain that it would help safeguard classified information by ensuring access only by Members deemed "trustworthy" and, thereby, limit the possibility of leaks and inadvertent disclosures. In addition, the clearance process itself might make recipients more conscious of and conscientious about the need to safeguard this information as well as the significance attached to it. As a corollary, supporters might argue that mandating a clearance to serve on a panel possessing classified information could increase its members' appreciation of the information's importance and its protection's priority. This, in turn, might help the committee members gain the access to information that the executive is otherwise reluctant to share and improve comity between the branches.

Opponents, by contrast, contend that security clearance requirements would compromise the independence of the legislature if an executive branch agency conducted the background investigation; had access to the information it generated; or adjudicated the clearance. Even if the process was fully under legislative control, concerns might arise over: its fairness, impartiality, objectivity, and correctness (if determined by an

inexperienced person); the effects of a negative judgement on a Member, both inside and outside Congress; and the availability of information gathered in the investigation, which may not be accurate or substantiated, to other Members or to another body (such as the chamber's ethics committee or Justice Department), if it is seen as incriminating in matters of ethics or criminality. Opponents might contend, moreover, that adding this new criterion could have an adverse impact on individual Members and the full legislature in other ways. Opponents also maintain that it might impose an unnecessary, unprecedented, and unique (among elected federal officials and court judges) demand on legislators; create two classes of legislators, those with or without a clearance; affect current requirements for non-Member access to holdings of committees whose own members might need clearances; possibly jeopardize participation by Members without clearances in floor or committee proceedings (even secret sessions); and retard the legislative process, while investigations, adjudications, and appeals are conducted.

Direct Senators or Senate Employees to Take or Sign a Secrecy Oath to Be Eligible for Access. This proposal would require a secrecy oath for Senators and staffers, similar to the current requirement for their House counterparts. An earlier attempt to mandate such an oath for all Members and employees of both chambers of Congress seeking access to classified information occurred in 1993; but it was unsuccessful. If approved, it would have prohibited intelligence entities from providing classified information to Members of Congress and their staff, as well as officers and employees of the executive branch, unless the recipients had signed a nondisclosure agreement — pledging that he or she "will not willfully directly or indirectly disclose to any unauthorized person any classified information" — and the oath had been published in the *Congressional Record*.[10]

Direct All Cleared Staff — or Just Those Cleared for the Highest Levels — to File Financial Disclosure Statements Annually. This demand might make it easier to detect and investigate possible misconduct instigated for financial reasons. And many staff with clearances may already file financial disclosure statements because of their employment rank or salary level; consequently, few new costs would be added. Nonetheless, objections might arise because the proposal would impose yet another burden on staff and result in additional record-keeping and costs. This requirement's effectiveness in preventing leaks or espionage might also be questioned by opponents.

Require Polygraph Examinations and/or Drug Tests for Staff to Be Eligible for Access to Classified Information. Under such proposals, tests could be imposed as a condition of employment for personnel in offices holding classified information, only on staff seeking access to such information, or for both employment and access.[11] Objections have been expressed to such tests, however, because of their cost and questionable reliability.

---

[10] *Congressional Record*, daily ed., vol. 139, August 4, 1993, pp. H5770-H5773; November 18, 1993, p. H10157.

[11] In the 105th Congress, the House approved a rule directing "the Speaker, in consultation with the Minority Leader, shall develop through an appropriate entity of the House a system for drug testing in the House ... (which) may provide for the testing of a Member, Delegate, Resident Commissioner, officer, or employee of the House...."